UNITED STATES DISTRICT COURT

DISTRICT OF SOUTH DAKOTA

SOUTHERN DIVISION

UNITED STATES OF AMERICA,	*	CR. 09-40130
Plaintiff,	*	
vs.	*	REPORT and RECOMMENDATION (Motion to Suppress)
JEREMY VINCENT NELSON,	*	
Defendant.	*	

Pending is Defendant's Motion to Suppress Evidence and Request for a *Franks* Hearing (Doc. 17). A hearing was held on Monday, March 29, 2010. Defendant was personally present and represented by his counsel of record Assistant Federal Public Defender Tim Langley. The Government was represented by Assistant United States Attorney Jeff Clapper. Knology employee Daryl Elcock and South Dakota Division of Criminal Investigation Agent Troy Boone testified at the hearing. Additionally, both parties have submitted briefs[1] and oral argument was heard at the conclusion of the hearing. Based on a careful consideration of all of the evidence, and counsel's written and oral arguments, the Court respectfully makes the following:

RECOMMENDATION

It is respectfully recommended that Defendant's Motion to Suppress be **GRANTED.**

JURISDICTION

Defendant is charged in an Indictment with Possession of Child Pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2256(8). The pending Motion to Suppress was referred to the Magistrate Judge pursuant to 28 U.S.C. § 636(b)(1)(B), Judge Piersol's Standing Order dated November 29, 2006 and Judge Schreier's Standing Order dated March 18, 2010.

[1]Supplemental briefs were submitted at the Court's request.

FACTUAL BACKGROUND

Troy Boone is the Task Force Commander for the State of South Dakota Internet Crimes Against Children Task Force. TR 30. He has been with the ICAC since 2006, and has been the Commander since November, 2009. *Id.* He has conducted approximately seventy child pornography investigations using file-sharing software. TR 31. He uses a database created by the Wyoming Division of Criminal Investigation which keeps a record of IP addresses where specific known child pornography images have been seen using file-sharing software. *Id.*

Agent Boone identified EX 4, which is a copy of the subpoena he prepared and forwarded to Knology to obtain information about IP address 216.16.82.227. He also identified EX 5, which is the affidavit in support of a search warrant he prepared for this case. TR 32. The Search Warrant Affidavit contains a paragraph which explains the importance of obtaining subscriber information for an IP address for the particular time the agent observes child pornography activity on the internet:

> I was able to identify a computer at an IP address that appeared to be offering files consistent with child pornography for distribution. This can be done as IP addresses are often a temporary number issued to a computer on a network and after the IP address is no longer in use it is reassigned to another computer. This is illustrated by ***having to subpoena an Internet Service Provider for an exact date/time*** pertaining to an IP address for an investigation.

See EX 5, p. 5.(bold italics added for emphasis).

On September 28, 2009, Agent Boone came across IP address 216.16.82.227 which was distributing child pornography. TR 32-33. He issued the subpoena to Knology to try to get subscriber information associated with that IP address. TR 33. The subpoena requested "subscriber information for IP address 216.16.82.227 on 9-28-09 at 00:46 (+0000) GMT to 9-28-09 at 00:29(+0000) GMT, including any and all billing information and payment information including credit card number, connection dates and times, and current IP address."[2]

[2]00:46 GMT means Grenwich Mean Time. Central Standard Time (daylight savings) is GMT -5:00. 00:46 GMT on September 28, therefore, translates to 7:46 p.m. CST on September 27, 2009. TR 58. It is apparent the Grenwich Mean Times are juxtaposed on the subpoena.

Knology responded to the subpoena in a series of emails. TR 33. *See* EX 2. The final email was dated October 12th, and included an attachment. TR 34. The attachment consisted of subscriber information including Jeremy Nelson's name, address, telephone number, account number, customer ID, and a DHCP log[3] for the dates October 6 and October 12, **but not for September 28**. TR 34-35, 38, EX 7. The email was from Knology employee Jason Griggs. The message of the October 12 email said "[h]ere is the info for the IP address "216.16.82.227" for the date of 10/06/09. The same user is assigned the same IP address today (also included in the log)." EX 2.

The September 28 DHCP log information was provided in an earlier email dated October 7 from Knology employee Cynthia Spence to Knology employee Jason Rang. TR 34, EX 2. The information in the October 7 email, which contained the DHCP log for September 28, was for a time frame at approximately 11:24 p.m. central time, **not the "time requested**," which was between 7:29 pm and 7:46 p.m. on September 27, 2009. TR 22. Rang replied to the October 7 Spence email asking "can the police provide a MAC address to see if it matchs (sic) the 00:1e:ee:2e:cc:36 address?" Spence replied asking Rang if the police had a suspected MAC address or were the police hoping Knology could provide it? Then Jason Griggs sent an email to Cynthia Spence informing her the police were looking for them to uncover the subscriber information. Cynthia told Griggs to let the police know Knology needed to know ASAP if "he" sent out any more "material" so they could check their logs again. On October 8, Griggs forwarded the MAC address information to Boone, and told him Knology was "still working on this one" and that "the offender" has not been online since the 28th and might be using a "spoofed" IP address. EX 2 p.1. Griggs asked Boone to notify Griggs immediately when "he" started his activity again. On October 9, Boone told Griggs (via email) that "he" had been on the system on October 3rd, 5th and 6th at specified times. On

[3]A DHCP is an acronym for dynamic host control protocol. A DHCP log is a log of connections to the internet by a certain internet subscriber, through an IP address which is assigned by the PC server. TR 13, 20. The DHCP log also tracks the MAC number of the hardware which is requesting access to the internet. TR 17. A MAC address is like a fingerprint for a person, except it is for a piece of equipment. *Id.* Every cable modem and PC or server or anything else that tries to access the internet has a MAC address. *Id.* In this case, the MAC address for Defendant's cable modem appeared as his "customer ID" number (00:1E:46:BE:D3:EC).TR 18, EX 3. The MAC number for the Defendant's computer was 00:1e:ec:2e:cc:36. TR 19, EX 3.

October 12th, Griggs sent the attachment containing the subscriber information identifying Jeremy Nelson, and attaching the DHCP logs for October 6 and 12. EX 2, p.1.

The statement in Agent Boone's affidavit to the issuing magistrate judge says "On October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by Jeremy Nelson at 616 ½ Locust Street, Yankton, South Dakota 57078 on the dates and times requested."[4] Although the "dates and times requested" were in actuality September 27, 2009 at 7:29-7:46 p.m.,[5] and although the October 12 email from Griggs only referenced October 6 and October 12, Agent Boone explained that he nevertheless included the critical paragraph in his affidavit because **"**[b]ased on what Knology had sent me in the email and the log file, and based on what I had seen on the IP address, I knew that–excuse me, on the IP history that I used for this case, I knew that there was only one computer that would be responsible for the distribution of the child pornography in this case. . . . Based on the IP . . . excuse me. . .the DHCP log that contained the MAC address of the modem, the MAC address of the computer, and based on the IP history that I had run through the Wyoming database, I knew that that particular computer was sharing pornography at one IP address and at one port number,[6] and sharing the same files over that 15 days time stretch from when I initially saw it to when I got the final subpoena results back from Knology." TR 36. He further testified that Knology's response to his subpoena (EX 2 & EX 7) "and also the IP history, and me looking at what the IP address had been doing on the Wyoming network–or the Wyoming database" in other words the information Knology provided plus additional information Boone had led him to write the critical paragraph. TR 42, 59, 65-66, 78-79.

---

[4]For the sake of brevity this paragraph will be referred to as " the critical paragraph."

[5]This is based on the conversion from GMT as requested in the subpoena to central standard time.

[6]Agent Boone explained that a port number is equivalent to a "channel" that a file-sharing program uses when it goes out and communicates with other file sharing programs on the internet. TR 50-51. In this instance, the IP address in question used the same port number (22662) each of the 172 times it distributed child pornography throughout the thirty-three day time period it was seen on the network. TR 51-52. Boone explained that "if it was the same port number at the same IP address, it was more than likely the same computer the whole time." TR 52.

On cross-examination, Agent Boone first testified Knology told him Jeremy Nelson was assigned IP address 216.16.82.227 on September 28. TR 63. When counsel read Griggs' October 12 email into the record, however, and added "so they tell you that Jeremy Nelson had this IP address on October 6 and October 12. They don't tell you that he's assigned address on September 28," Boone responded, "Well, I knew that based on the previous emails." TR 64. Boone also explained, "I knew on the 12th that on the 28th the same person had the same computer at the same IP address with the same MAC address, as they did on the 6th and the 12th. That's why when I applied for the search warrant, I indicated that in there, that it's the same IP address, and I also included this string of emails with the evidence CD that I made showing the link between the 28th, the 6th, and the 12th." TR at 65-66. Boone conceded, however, he did not include any of the information about the MAC address in his affidavit. TR 67. Boone steadfastly asserted that if he would have any question his statement was incorrect, he would never have applied for a search warrant. TR 71.

Boone testified that between September 28, 2009 and October 31, 2009, IP address 216.16.82.227 offered 172 files for distribution which are known by law enforcement to be child pornography. TR 47-48.

Daryl Elcock testified as the corporate representative of Knology. TR 9. He was not one of the Knology employees involved in responding to Boone's subpoena, but he is the Network Manager for the Sioux Falls Division which includes Yankton. TR 9-10. He is responsible for maintaining the network from the customer tap, onto the core of the network, and onto Knology's internet peers. *Id.* Mr. Elcock only became involved in this case one week before the suppression hearing. TR 29. Elcock identified EX 1, business records gathered and certified by Jason Griggs. TR 11. Griggs is the Security/Fraud Coordinator and Legal Compliance Officer. *Id.* Griggs is physically located in West Point, Georgia. TR 14. Griggs collected information and corresponded with his co-workers after Boone subpoenaed information about IP 216.16.82.227. Griggs then forwarded the email sequence to Mr. Elcock. TR 14. Mr. Elcock offered the technical explanations contained in footnote 3 regarding the meaning and significance of the terms DHCP log and MAC address , among other things. TR 12-13.

Elcock explained that EX 3 (a compilation of the DHCP logs for September 28, Oct. 6 and Oct. 12) was pulled together and put on the same piece of paper "shortly after the subpoena" but he was not aware of who gathered the information or why the document had not been revealed until the date of the evidentiary hearing. TR 22. The times reflected on EX 3 represent central standard time. TR 22. Mr. Elcock agreed that when, on October 7, Cynthia Spence viewed the September 28 DHCP logs for the pertinent IP address, Knology "still didn't know who it is." TR 25. She indicated Knology would just have to continue to monitor to see if the person got back online. TR 25. He also agreed that when, on October 12, Knology provided information to Troy Boone about the name and address of who was associated with the subject IP address, no information about September 28 was included. TR 26. Elcock also agreed that "after all of the discussion back and forth, what Troy Boone finally gets from Knology is based exclusively on the connection of the IP address with Jeremy Nelson on October 6 and October 12, Correct?" TR 28.

DISCUSSION

Burden of Proof

As a general rule, the burden of proof is on the defendant who seeks to suppress evidence, *United States v. Phillips,* 540 F.2d 319 (8th Cir.1976), but on the government to justify a warrantless search or seizure. *United States v. Bruton*, 647 F.2d 818 (8th Cir.1981). The standard of proof is a preponderance of the evidence. *Lego v. Twomey*, 404 U.S. 477, 92 S.Ct. 619, 30 L.Ed.2d 618 (1972). Additionally, to become entitled to an evidentiary hearing to attack the veracity of a search warrant affidavit, the defendant must "allege deliberate falsehood or reckless disregard for the truth, and support the allegations with an offer of proof." *United States v. DeBuse*, 289 F.3d 1072, 1074 (8th Cir. 2002) (citation omitted).

1. Franks Hearing

"A defendant is entitled to a hearing to determine the veracity of a search warrant affidavit if he . . . can make a substantial preliminary showing that a false statement was included in the affidavit (or that relevant information was omitted from it) intentionally or recklessly, and that the allegedly false statement was necessary to a finding of probable cause or that the alleged omission would have made it impossible to find probable cause." *United States v. Mathison*, 157 F.3d 541,

547-48 (8th Cir. 1998) (citations omitted). The requirement for a substantial preliminary showing is "not lightly met." *United States v. Wajda*, 810 F.2d 754, 759 (8th Cir. 1987). A mere allegation in the absence of an affidavit of a witness or some other form of corroboration that the false statement was made knowingly, intentionally, or with reckless disregard for the truth, is insufficient to make the difficult preliminary showing. *Mathison*, 157 F.3d at 548, *quoting Franks*, 438 U.S. at 171, 98 S.Ct. at 2674. As explained in *Mathison*, merely identifying what one claims are the specific falsehoods in the affidavit without offering proof that the alleged falsehoods were deliberate or reckless is not enough. "When no proof is offered that an affiant deliberately lied or recklessly disregarded the truth, a *Franks* hearing is not required." *Mathison*, 157 F.3d at 548 (citations omitted).

In this case, the Defendant presented evidence produced in discovery (received as EX 2 and EX 7 during the evidentiary hearing) which on its face suggested that Knology did not provide any information about who was assigned to IP address 216.16.82.227 on the "dates and times requested" (September 27, 2009 between 7:29 p.m. and 7:46 p.m.) but instead provided subscriber information for two entirely different dates (October 6 and October 12). The critical paragraph in Boone's affidavit ("On October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St. Yankton, SD 57078 on the dates and times requested") is the only paragraph in the affidavit which ties the Defendant to the IP address, and therefore the only paragraph which provides probable cause to search the Defendant's home. Combined with the paragraph in the search warrant affidavit which explains the importance of "having to subpoena an Internet Service Provider for an exact date/time pertaining to an IP address for an investigation," the Defendant met his preliminary burden of making a substantial showing (1) that a false statement was intentionally or recklessly included in the affidavit; and (2) that the allegedly false statement was necessary to the finding of probable cause.

2. Motion to Suppress

"[A] search warrant must be voided and the fruits of the search suppressed if a defendant proves by a preponderance of the evidence that (1) a law enforcement officer knowingly and intentionally, or with reckless disregard for the truth, included a false statement in the warrant

affidavit, and (2) without the false statement, the affidavit would not have established probable cause." *United States v. Neal*, 528 F.3d 1069, 1072 (8th Cir. 2008) (*citing Franks*, 438 U.S. at 155-56). This case is difficult, because it was obvious during the evidentiary hearing that Agent Boone was and is thoroughly convinced that there is no possibility the computer which was distributing child pornography on the "dates and times requested" belonged to anyone other than Jeremy Nelson. That, however, is not the issue this Court has been asked to decide. The task at hand is whether Boone provided *sufficient truthful information in his affidavit* to allow a neutral, detached magistrate judge to reach the same conclusion.

The critical paragraph ("On October 12, 2009, **Knology responded with information stating** that IP address 216.16.82.227 was subscribed to by Jeremy Nelson at 616 ½ Locust Street, Yankton, South Dakota 57078 **on the dates and times requested**") is false. First, Knology did not provide any information about the "dates and times requested" because the "dates and times requested" were actually September 27, 2009 between 7:29 p.m. and 7:46 p.m.–a time frame about which Knology provided absolutely no information. Second, it became clear during the evidentiary hearing that Knology provided the subscriber information identifying Jeremy Nelson, but **it was Agent Boone, not the Knology employees, who pieced together the information** provided by Knology (along with other independently gained information) to finally determine it was Jeremy Nelson who subscribed to the IP address on "the dates and times requested."

Knology provided the raw data, but Boone performed the calculations, so to speak.[7] Boone acknowledged as much during his testimony. Although he testified "they told me that on the 28th Jeremy Nelson had that IP address" (TR at 37) he qualified his statement when he further explained that it was the combination of information received from Knology, along with Boone's own research, training and experience which allowed him to reach the conclusion there was only one computer in

[7]It remains unclear why Knology could not figure out Jeremy Nelson was the subscriber until after Boone provided Knology with information instead of vice versa. Interestingly, as of October 8th, Jason Griggs reported to Boone that Knology was "still working on it" and that it did not appear the "offender" had been online since September 28th. Only after Boone replied and informed Griggs "he" had in fact been online on October 3, 5 and 6 was Griggs able to produce the DHCP logs for October 6 and 12, and the "info for the IP address . . for the date of 10/6/2009 . . [and] today."

the world that could have been associated with that IP address at those dates and times. TR 70. *See also* TR 75-76.[8] Agent Boone did not inform the magistrate judge, however, that *he* not Knology determined Nelson was the subscriber on "the dates and times requested" nor did he explain to the magistrate judge how he reached his conclusion.[9] The distinction is fine, but important. "The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from the evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14, 68 S.Ct. 367, 92 L.Ed. 436 (1948). "It follows that a police officer cannot make unilateral decisions about the materiality of information, or, after satisfying him or herself that probable cause exists, merely inform the magistrate judge of inculpatory evidence." *Wilson v. Russo*, 212 F.3d 781, 787 (3rd Cir. 2000). The Eighth Circuit has noted a fact is omitted from an affidavit with reckless disregard for the truth if "any reasonable person would have known that this was the kind of thing the judge would wish to know." *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993). Any reasonable person would have known that the magistrate judge would have wished to know that even though Boone subpoenaed Knology

---

[8]The following exchange between defense counsel and Boone is enlightening: **Q:** Agent, isn't it your testimony that you came to the conclusion that Jeremy Nelson–if Jeremy Nelson had this IP address on October 6 and October 12, if Knology is telling you that's the name of the guy on the 6th and the 12th of October, you believe there's enough information to conclude he must have been the guy on the 28th? **A: Absolutely, or I wouldn't have put it in the Affidavit. Q:** But is it not true that Knology did not tell you that. You figured it out, you believe, from the data they provided you. **A: I figured it out. Correct. Q:** And you didn't explain that sequence of events or your thinking on the MAC addresses or account for the three different MAC addresses to the Judge. Didn't you just tell the Judge, "Knology told me Jeremy Nelson was the guy that had this IP address on the 28th of September." Isn't that what you told the Judge? **A: That's exactly what I told the Judge.**

[9]All of this information was provided to the Defendant in discovery, and was explained in more than sufficient detail to persuade this magistrate judge during the evidentiary hearing that probable cause to search existed. Again, the issue is not whether there was probable cause to search or whether sufficient evidence of probable cause was presented during the evidentiary hearing. Instead the issue is whether Boone's affidavit contained sufficient truthful information to support a probable cause determination by a neutral, detached magistrate judge. "Under the cases of this Court, an otherwise insufficient affidavit cannot be rehabilitated by testimony concerning information possessed by the affiant when he sought the warrant but not disclosed to the issuing magistrate. *See Aguilar v. Texas*, 378 U.S. 108, 109 n. 1, 84 S.Ct. 1509, 1511, 12 L.Ed.2d 723. A contrary rule would, of course, render the warrant requirements of the Fourth Amendment meaningless." *Whitely v. Warden, Wyoming State Penitentiary*, 401 U.S. 560, 564, n.8, 91 S.Ct. 1031, 1035, n.8, 28 L.Ed.2d 306 (1971).

requesting subscriber information relating to an IP address on September 27, 2009 for a specific period of time between 7:29 p.m. and 7:46 p.m., ("the dates and times requested,") the response Boone received contained an attachment which referred specifically only to October 6 and October 12. Any reasonable person would have also known the magistrate judge would have wished to know that it was Boone, not Knology, who figured out, based on information received from Knology along with other information, that Nelson was the subscriber on the "dates and times requested," and that the magistrate judge would have wished to know how Boone reached such a conclusion. For these reasons, Boone's **assertion in the affidavit that it was Knology who stated** the identity of the subscriber, and his **omission from the affidavit that it was Boone himself,** who concluded Nelson was the subscriber on the "dates and times requested" rises above negligence to the level of a reckless disregard for the truth.

An affirmative statement is made with reckless disregard for the truth if "when looking at all the evidence available to the officer, the officer must have entertained serious doubts as to the truth of his . . . statements or had obvious reasons to doubt the accuracy of the information he . . . reported." *United States v. Neal*, 528 F.3d 1069, 1072 (8th Cir. 2008). Boone had no doubt Nelson subscribed to the IP address on "the dates and times requested. " But in light of his admission that **he** (Boone) "figured it out" by combining information from Knology together with his own research and together with his own training and experience, he had obvious reasons to doubt the accuracy of his statement to the magistrate judge that " . . .***Knology*** responded with information stating that IP address 216.16.82.227 was subscribed to by Jeremy Nelson at 616 ½ Locust Street, Yankton, South Dakota 57078 ***on the dates and times requested***." For these reasons, Boone's statement in the critical paragraph rises above mere negligence to the level of a reckless disregard for the truth.

The critical link connecting the subscriber information on October 6th and October 12th to the same IP address which is referenced to the September 28th log information (and then yet another link must be made to the September 27th time frame for which there are no DHCP logs at all) was not explicitly made anywhere except inside Agent Boone's head. While it is not doubted that Boone's conclusions are correct and his intentions were good, by failing to inform the magistrate judge that Knology could not quite put the pieces of the puzzle together but he (Boone) could, the end result

was to exclude the power of the *magistrate judge* from the process to make the probable cause determination and to substitute instead the conclusion of the investigating officer. "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *United States v. Stanert*, 762 F.2d 775, 782 (9th Cir. 1985) (*citing Illinois v. Gates*, 462 U.S. 213, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).

Because the statement which provided the link between the IP address and Jeremy Nelson was false and because it was made with reckless disregard of the truth, the next step is to excise the false statement from the affidavit to "then determine whether, absent the false material or supplemented with the omitted material, the affidavit's remaining contents are sufficient to establish probable cause . . . If the remaining contents are insufficient to establish probable cause, the warrant must be voided and the evidence or statements gathered pursuant to it excluded." *United States v. Clapp*, 46 F.3d 795, 799 (8th Cir. 1995) (citations omitted). In this case, the critical paragraph is the only paragraph which makes the crucial connection between the Defendant and the IP address which was distributing the child pornography on the dates which are mentioned in the search warrant. The remaining contents, therefore, are not sufficient to establish probable cause to search Jeremy Nelson's home at 616 and ½ Locust Street in Yankton, SD. The evidence gathered pursuant to the warrant, therefore, should be suppressed.

The Court has not reached this conclusion without qualms. Agents cannot be permitted, however well-intentioned, to subvert the constitutional requirement of a warrant supported by oath or affirmation by recklessly disregarding the truth, no matter how confident they are in their own beliefs. *See United States v. Scully*, 1992 WL 159329 (N.D. Ill.). Judge Eisele made a similarly difficult decision when he invalidated a warrant because the agent procured, but did not include in his affidavit, the appropriate information in a warrant application:

> So we have here a case where able law enforcement officers had, through their investigation, clearly obtained sufficient information to support the search warrant they sought, but they failed to properly bring this information before the magistrate. There is no evidence of any intent to deceive. But, we have here more than simple

> negligence. There was reckless disregard in failing to carefully read the draft of the affidavit to be sure that the information provided was true and adequate to support a finding of probable cause.

United States v. McKey, 2007 WL 2601206 (E.D. Ark.). at *6. Similarly, Agent Boone is an able law enforcement officer who clearly possessed sufficient information to support the search warrant he sought. There is no evidence he intended to deceive anyone. To write off his failure to acknowledge that it was he himself, not Knology who concluded it was Jeremy Nelson who subscribed to the IP address on the "dates and times requested" as mere negligence, however, would obliterate the fine but important distinction drawn by the Fourth Amendment— law enforcement agents may not make unilateral decisions about probable cause, instead sufficient information must be provided to allow the probable cause determination to be made by a neutral, detached magistrate judge. *Illinois v. Gates*, 462 U.S. 213, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).

Finally, the good faith exception as defined in *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 does not apply according to the terms of the *Leon* case itself. "The deference accorded to a magistrate's finding of probable cause does not preclude inquiry into the knowing or reckless falsity of the affidavit on which that determination was based." *Id.* 468 U.S. at 914, 104 S.Ct. at 3416. *See also, United States v. Gipp*, 147 F.3d 680, 688 (8th Cir. 1998) (noting good faith exception does not apply if affiant made intentional or reckless misstatements).

CONCLUSION

For the reasons more fully explained above, it is respectfully RECOMMENDED to the District Court that Defendant's Motion to Suppress Evidence and for a Franks Hearing (Doc. 17) be GRANTED.

NOTICE TO PARTIES

The parties have fourteen (14) days after service of this Report and Recommendation to file written objections pursuant to 28 U.S.C. § 636(b)(1), unless an extension of time for good cause is obtained. Failure to file timely objections will result in the waiver of the right to appeal questions of fact. Objections must be timely and specific in order to require de novo review by the District Court.

Thompson v. Nix, 897 F.2d 356 (8th Cir. 1990)

Nash v. Black, 781 F.2d 665 (8th Cir. 1986)

Dated this 23rd day of April 2010.

BY THE COURT:

s/John E. Simko

John E. Simko
United States Magistrate Judge